A PARTE ESPECIAL DO CÓDIGO PENAL BRASILEIRO FRENTE À CRIMINALIDADE NA INFORMÁTICA

Nelson Burin Neto
Bacharel em Direito pela ITE.
Ex-estagiário do Ministério Público.
Advogado militante em Botucatu.

RESUMO

O trabalho destina-se a apreciar a amplitude das condutas típicas atreladas ao âmbito informático presentes na Parte Especial do Código Penal brasileiro. Através do mesmo, busca-se evidenciar o raio de incidência das normas penais incriminadoras, analisando o alcance destas, sem, contudo, olvidar-se daquelas ações que remanescem à míngua de uma tipificação legal, face ao surgimento de novos bens jurídicos a serem tutelados e ao ineditismo conferido à atuação dos delinqüentes, propiciados pelo avanço informático. Ao término, após extensa investigação doutrinária, norteando-se, exclusivamente, pelo método de pesquisa científico, conclui-se que, mesmo havendo a possibilidade da Parte Especial do Código Penal de 1940 ser aproveitada em muitos casos, é inegável a premência em se "criminalizar" alguns comportamentos, até então, tidos como atípicos, visando a preencher as lacunas existentes.

Palavras-chave: código penal; parte especial; crimes de informática; abrangência.

1. INTRODUÇÃO

Nos dias hodiernos, testemunhamos a era da informação, a qual carreou e vem acarretando alterações significativas ao próprio agir humano. Neste passo, o correio eletrônico passou a concorrer com a secular comunicação postal. Igualmente, operações comerciais e bancárias, outrora presenciais, transportaram-se para os domicílios onde se verifica a presença de um computador e um *modem*. De maneira análoga, a pesquisa e a leitura eletrônica desbancaram a supremacia do papel-celulose.

No mundo do crime, não foi diferente. Os transgressores da lei penal logo viram no computador e na Internet formidáveis instrumentos à consecução de vários delitos. Como se não bastasse, essa revolução tecnológica também deu azo à criatividade delituosa, gerando comportamentos inéditos que, não obstante o alto grau de reprovabilidade social, ainda permanecem atípicos.

O Direito, por sua vez, tendo como função primordial definir parâmetros que orientem o comportamento humano em todas as esferas, inclusive no âmbito informático, evidentemente caminha atrás de toda essa realidade "virtual".

Mas em que medida a legislação penal vigente está preparada para enfrentá-la? Seria realmente necessário recorrer ao Direito Penal tipificando-se condutas específicas, caracterizadoras dos crimes informáticos? Os recursos da exegese jurídica seriam a panacéia para o problema inerente à tipicidade?

Diante de tal quadro, o objetivo geral do presente ensaio será uma avaliação atinente à amplitude de incidência das condutas típicas constantes da Parte Especial do Código Penal brasileiro, com vistas à necessidade de "criminalização" dos comportamentos atípicos que permeiam o meio informático.

2. REVOLUÇÃO TECNOLÓGICA E CRIMINALIDADE

Nos tempos modernos, é um equívoco pensar que os computadores podem ser utilizados apenas como máquinas de escrever de última geração. Diariamente, os micros apresentam novas utilidades, sendo intricado prever todos os avanços que poderão ocorrer nesse campo nos próximos anos, haja vista a velocidade com que as evoluções tecnológicas se dão.

É, justamente, a partir dessa abrupta evolução da informática que surge a relação entre tecnologia e criminalidade.

A informática, com tudo o que representa em termos de aprimoramento, também se mostra como notável instrumental para a delinqüência, tornando-a moderna e sofisticada. Se não vejamos.

Ao viabilizar o acesso à "grande rede", o provedor propicia ao usuário, o qual pode perfeitamente ser um criminoso contumaz, inúmeras facilidades, tais como: a possibilidade de se contatar, numa velocidade incrível, com demais transgressores da lei penal (eventuais "comparsas" que se encontrem em países distantes), bem como atrair vítimas em potencial.

Perfilhando essa linha de raciocínio, forçoso reconhecer que, assim como as transações comerciais se aprimoraram com a criação da Internet, o mesmo pode se dar com eventuais negociações entre criminosos.

Nesse diapasão, visando a reforçar as ilações adrede lançadas, pode-se certificar a existência de determinadas tendências no tocante ao emprego da Internet pelas organizações criminosas.

A primeira delas condiz com a utilização da Internet para a prática de atividades fraudulentas. Não seria de todo inverossímil vislumbrarmos a possibilidade de um indivíduo conhecedor de comandos informáticos associar-se ao crime organizado, assessorando este em suas manobras delituosas.[1]

Outra vertente a ser declinada é que à medida que o crime organizado afasta-se das suas atividades habituais e concentram-se, progressivamente, em oportunidades de crimes financeiros ou de "colarinho branco", as atividades baseadas na Internet tornar-se-ão ainda mais prevalecentes por estes criminosos.[2]

Todavia, tal alusão não implica assegurar que o crime organizado alterará o âmago de suas peculiaridades. Seu inerente feitio em utilizar a força e a intimidação também se coaduna com o incremento de esquemas sofisticados da "ciberextorsão". É razoável imaginar que a partir dos recursos informáticos, tal gama de criminosos, interagindo com *experts* da área, passe também a chantagear eventuais vítimas ou desafetos, no sentido de romper sistemas de informação e comunicação, bem como aniquilar dados.

Analisando-se sob esse mesmo flanco, outra empreitada criminosa relativa a essas organizações sobressalta-se: a Internet pode ser, vertiginosamente, utilizada

1 Exemplo de extrema notabilidade ocorrera em outubro de 2000 e referiu-se ao Banco da Sicília. Um grupo de aproximadamente vinte indivíduos, sendo alguns membros de famílias mafiosas, ao "trabalharem" com um funcionário interno da referida instituição financeira, criaram um clone digital do componente *online* do banco. Planejaram, então, utilizá-lo para desviar cerca de US$ 400 milhões alocados pela União Européia para "projetos" regionais na Sicília. O dinheiro seria lavado através de diversas instituições financeiras, que incluíam o Banco do Vaticano e bancos na Suíça e em Portugal. Felizmente, o esquema foi frustrado quando um integrante do grupo delatou todo o esquema às autoridades, revelando para estas, que o crime organizado antecipa enormes oportunidades de lucro derivadas do crescimento dos bancos eletrônicos e do comércio eletrônico. (WILLIAMS, 2001)

2 Durante o final da década de 1990, constatou-se a ocorrência de casos envolvendo organizações criminosas que manipulavam ações de pequenas empresas utilizando a clássica técnica de "forçar alta e vender". Para tanto, a Internet foi utilizada para disseminar informações que "inflassem", artificialmente, o preço das ações. Dentre os envolvidos, encontravam-se membros das famílias criminosas Bonnano, Genovese e Colombo, bem como membros imigrantes russos do grupo de crime organizado. (WILLIAMS, 2001)

para "lavagem de dinheiro". Afinal, é inconteste que os leilões *on line*, por exemplo, fomentam a possibilidade de se movimentar dinheiro através de compras aparentemente legítimas.

Desta feita, forçoso perfilhar que a "sintonia" entre o crime organizado e a Internet está disposta a prosperar, ainda mais, no futuro. A utilização desvirtuada da Internet fornece caminhos para o crime, permitindo, assim, uma exploração voltada para ganhos ilícitos abundantes com um grau reduzidíssimo de risco. Praticamente, uma "panacéia" para o crime organizado.

Em suma, o computador, além de se tornar um meio "eficaz" para diversas práticas delitivas, (afinal, crimes como o favorecimento da prostituição, incitação a crime, estelionato, racismo, pedofilia, dentre outros "ganharam fôlego" no ciberespaço) veio, também, facilitar, ainda mais, a vida dos criminosos, conferindo-lhes, muitas vezes, não só comodidade, mas também a segurança e agilidade nem sempre presentes no *modus operandi* usual de vários delitos.

3. SISTEMAS DE CLASSIFICAÇÃO

Estudos sistemáticos e científicos sobre a matéria remontam da década de 70, ocasião em que através de métodos criminológicos, passou-se a analisar, ainda que em número reduzido, os crimes praticados através de computadores (FERREIRA, 2001).

Reafirmando a premência no combate a essa espécie de criminalidade, a doutrina contemporânea, apesar de tímida, vem demonstrando certa preocupação no que tange à progressão de tais delitos, de modo que hoje, relativamente à classificação dessas condutas, ainda, não há um consenso.

Os sistemas mais comuns representam propostas baseadas na distinção entre os crimes tradicionais cometidos por meio de computadores e, noutra categoria, as demais ações de abuso de informática, específicas dessa área.

Nesses moldes, reputa-se como a categorização mais completa aquela propugnada por Jesus (2000 apud ARAS, 2001, p. 10), o qual entende que os crimes de informática podem ser **puros ou próprios** e **impuros ou impróprios**.

Consoante o entendimento deste jurista, serão puros ou próprios aqueles em que o sujeito ativo visa, especificamente, ao sistema de informática em todas as suas formas, devendo-se entender estas como os elementos que compõem a informática, ou seja, o *software*, o *hardware*[3] (computador e periféricos), os dados e sistemas contidos no computador, os meios de armazenamento externo, tais como fitas, disquetes etc.

3 "*Hardware* constitui os componentes físicos do computador e seus acessórios. Exemplo: mouse, teclado, monitor etc. *Software* designa qualquer programa ou conjunto de programas e procedimentos referentes ao sistema de processamento de dados." (COSTA, 2003, p. 221-223)

Já os crimes eletrônicos impuros ou impróprios seriam aqueles em que o sujeito ativo se utiliza do computador como meio para atingir o resultado naturalístico, que ofenda o mundo físico, ou seja, ameaçando ou lesando outros bens, não-computacionais ou diversos da informática.

Desta feita, extrai-se o seguinte **conceito** para a expressão **crimes informáticos ou de informática**: são condutas típicas e antijurídicas em que o meio de execução ou o bem juridicamente protegido seja um objeto tecnológico da informática, assim compreendidos todos os componentes de um sistema de computação (*hardware*, redes, *software* etc.), e bem assim os dados eletronicamente tratados.

4. SUJEITO ATIVO

O agente criminoso que se utiliza da informática distingue-se dos demais pelo fato de fazer pleno uso do intelecto, bem como dos conhecimentos técnicos necessários para operar com destreza um computador.

Aprofundando-se na questão do perfil, segundo os apontamentos de Miranda (1999) a conduta de um típico delinqüente informático se desenvolveria em três estágios: primeiramente, o desafio, depois o dinheiro extra e, por fim, sustentar os altos gastos e o comércio ilegal.

Na verdade, essa descrição se enquadra no famoso termo *hacker*. Além dos *hackers*, meros invasores que agem apenas pelo desafio de sobrepujar e expandir suas habilidades nessa área, sem, contudo, provocarem prejuízos de maiores montas, existem os *crackers*, também denominados de "piratas eletrônicos" ou "*hackers* do mal". Estes se distinguem dos *hackers,* porquanto utilizam seus conhecimentos técnicos para quebrarem os dispositivos de segurança de redes de computadores, bem como invadirem os sistemas destes visando a subtrair informações estratégicas ou obter algum outro tipo de vantagem.

Ao lado destes há, ainda, os *lammers*, que, pelo fato de serem iniciantes, fazem o uso anti-social da rede, visando, tão-somente, a perturbar os demais usuários.

Nesta mesma senda, destaque-se que os delitos cometidos via Internet também são conhecidos pela denominação *special oportunity crimes*, ou seja, crimes afetos à oportunidade. Muitas vezes, os criminosos têm sua ocupação profissional ligada à área de informática, ou são pessoas que, de alguma forma, convivem constantemente com computadores. Dito isso, tem-se que uma outra espécie de agente vem tomando espaço na órbita da criminalidade virtual. Tratam-se dos *insiders*. Em síntese, nada mais são do que *hackers* internos de uma empresa.

Dignas ainda de realce são as figuras dos *cyberpunks* e *cyberterrorists*, os quais, almejando sabotar redes de computadores ou provocar a queda dos sis-

temas de grandes provedores, impossibilitam o acesso de outros usuários provocando, por conseguinte, detrimento econômico (ARAS, 2001).

Lamentavelmente, todos esses condenáveis atos efetivados através da Internet, contam, ainda, com dois fatores extremamente atraentes, quais sejam: a **instantaneidade** e o **anonimato**.

O certo é que para a elaboração de normas precisas, capazes de enquadrar toda e qualquer ação virtual perniciosa, impedindo um fator tão atrativo e presente naquelas condutas, até então atípicas, qual seja, a impunidade, é imprescindível avaliar o comportamento, a intenção e a mentalidade do agente, vez que só tal análise viabilizará a distinção entre os diversos tipos de condutas nessa área.

5. A RELATIVA INCIDÊNCIA DAS CONDUTAS TÍPICAS ATRELADAS AO ÂMBITO INFORMÁTICO

Considerando-se que a Parte Especial do Código Penal Brasileiro data de 1940, e que o computador aportou neste país, tão somente, em meados de 1960, é plausível inferir que esse conjunto de dispositivos mostra-se insuficiente e inadequado para suplantar todos os abusos no setor informático.

A pedra angular dessa ilação reside, pois, no problema relativo à tipicidade. Esta é, sem dúvida alguma, um dos maiores obstáculos à apuração e repressão das inúmeras condutas indesejáveis perpetradas através de computadores.

A colocação da contenda, nestes termos, ou seja, a partir dos ditames da tipicidade e, por conseguinte, dos imperativos oriundos da reserva legal, tem grande valia sim. Se não vejamos.

Em se tratando de informática e da Internet, deparamo-nos com delitos já tipificados pelo ordenamento jurídico penal, embora executados de maneira distinta (inovação no *modus operandi*). O avanço tecnológico possibilita certas peculiaridades no *modus operandi*, de maneira que a linha divisória entre os crimes de informática (impróprios) e os crimes comuns reside na utilização do computador para lograr êxito na empreitada criminosa. Analisando-se sob esse prisma, os crimes comuns também são perpetrados através de um meio que enseje o resultado naturalístico.

Concomitantemente, defronta-se com uma nova criminalidade, a qual atinge novos valores sociais. Daí a razão de utilizarmos a expressão relativa para designar a abrangência das normas penais vigentes. Estas serão aplicáveis, tão-somente, àquelas condutas que atinjam bens jurídicos já protegidos (dentre os quais, interpretando-se progressivamente alguns dispositivos, enquadra-se o sistema de informática).

5.1 Crimes de informática previstos no Código Penal brasileiro

5.1.1 Crimes contra a honra

Tanto a calúnia quanto o crime de difamação são passíveis de serem perpetradas através da Internet, isto é, em conversas *on-line*, bem como em *homepages.* É perfeitamente possível que uma pessoa "construa" uma *homepage* e nela atribua um fato ofensivo à honra de outrem. Aqui, o delito consuma-se, pois uma *homepage* pode ser visitada por qualquer pessoa conectada à Internet, permitindo, com isso, que qualquer outro "internauta" conheça as ofensas (CASTRO, 2003).

Com relação às ofensas enviadas por *e-mail*, temos que: se só a vítima utiliza-se do correio eletrônico, a consumação do delito torna-se difícil. O mesmo não pode ser dito quando se tratar de um *e-mail* conjunto[4] e o agente tiver conhecimento desta condição.

Vejamos, agora, o delito de injúria. Para a sua consumaçã,o é suficiente que o ofendido tome conhecimento do fato. Logo, tal crime pode ser cometido não só nas *homepages, nos sites,* nas salas de conversas *on-line,* mas também, através de um *e-mail* enviado, diretamente, à vítima.[5]

Digno de menção é que em casos de *chats,*[6] listas de discussão em geral, bem como na remessa simultânea de *e-mails* a diversos destinatários através dos recursos fornecidos pelo O*utlook,*[7] principalmente, ao se solicitar o reenvio a terceiros, incidirá a causa de aumento de pena de um terço inserta no artigo 141, inciso III, do Código Penal, conquanto se constituem meios inequívocos que facilitam a divulgação da calúnia, da injúria ou da difamação.

Em se tratando de mensagem eletrônica que veicule calúnia, seu encaminhamento a terceiros, por destinatário que sabe ser falsa a imputação, sujeitá-lo-á à incursão no artigo 138, § 1º, do Código Penal. O mesmo pode ser dito para aquele destinatário que reproduzir mensagem dessa natureza em sua *homepage* pessoal ou em *site* sob sua responsabilidade, uma vez que, de igual modo, divulgou a calúnia. (FELICIANO, 2001)

Saliente-se, por fim, que a mera dúvida sobre a veracidade das informações não elide a responsabilidade penal do destinatário, devido à existência da figu-

4 É o caso, por exemplo, de um *e-mail* utilizado por todos os integrantes de uma família.

5 Acrescente-se que *sites* comuns, *e-mails*, listas de discussão, a despeito de sua relativa publicidade, não são reputados meios de informação e divulgação para os fins do artigo 12, parágrafo único, da Lei n.º 5.250/67 (Lei de Imprensa). Assim, em hipóteses referentes à veiculação pela WEB não consistentes em meios de informação e divulgação aplicar-se-ão os dispositivos do Capítulo V, do Título I, da Parte Especial do Código Penal brasileiro.

6 Consiste num "modo de comunicação direta entre usuários de redes de informática, um diálogo textual, em tempo real." (CASTRO, 2003, p. 219)

7 Trata-se de um programa de correio-eletrônico da *Microsoft.*

ra do dolo eventual. Da mesma forma, não a afastará se, por ventura, alegar no corpo do *e-mail* em que segue a mensagem de caráter caluniador, não acreditar na informação veiculada (FELICIANO, 2001).

5.1.2 Ameaça

A conduta nuclear do tipo é ameaçar, ou seja, intimidar, prometer malefícios. A lei, por sua vez, não elenca formas especiais para a sua prática. Assim, o agente pode utilizar-se de uma *homepage* ou de *site*, no afã de nele inserir um texto de conteúdo ameaçador. De igual modo, o computador será o instrumento para a prática desta infração penal, quando o sujeito ativo valer-se de um *e-mail* ou salas de conversas *on-line* para tanto.

Oportuno consignar que a ameaça, ou seja, o mal prenunciado deve ser grave, a ponto de incutir temor no homem médio. Daí o porquê de ameaças jocosas, quando enviadas por *e-mail,* não configurarem o delito sob análise.

5.1.3 Furto

Como já visto anteriormente, o crime de informática pode ser praticado contra o sistema de informática ou através do mesmo.

No crime de furto, em especial, é possível observar as duas modalidades. Se o agente subtrai o computador ou um de seus acessórios, tal delito, em tese, será contra o sistema de informática. É o caso, por exemplo, de um sujeito que furta um *mouse*[8] de outrem. De outro lado, se o agente utilizar o computador para retirar valores de uma instituição financeira, a informática se mostrará como mero instrumento para a prática delituosa.

O exame da matéria, tendo como faceta o delito de furto, suscita questão interessantíssima relativamente à possibilidade de se furtar um *software*.

Parece-nos lógico definir furto de *software* como sendo a subtração do programa que esteja instalado no computador, o que, por sua vez, difere-se da reprodução, a qual consubstancia a popular figura da "pirataria". A hipótese, contudo, a princípio, tem relevância puramente acadêmica, vez que, em tese, a única maneira de subtrair um programa, sem reproduzi-lo, é subtraindo a máquina que o contém (FELICIANO, 2001).

É, contudo, plausível encontrarmos defensores de que há distorções entre a figura do *software,* erigido a obra de cunho intelectual, e o objeto material do delito de furto, qual seja, coisa alheia móvel.

8 Dispositivo que auxilia no manuseio do sistema, principalmente sistemas gráficos. O movimento que você faz com o mouse, é refletido na tela. É o auxiliar indispensável do teclado.

Pois bem. Muitas vezes, dentre os bens subtraídos encontram-se Compact Discs (CD´s) musicais. Ora, nesses casos, tais bens são considerados objeto material deste delito e, portanto, detentores de valor econômico; não obstante, contenham obra de caráter intelectual. Por conseguinte, seria um verdadeiro retrocesso jurídico, se assim não considerarmos o *software* instalado no interior de um microcomputador, ou mesmo programas contidos em disquetes ou CD´s. Veja-se que o valor de um CD musical se deve, inegavelmente, pelo conteúdo da obra nele contida. Entendimento diverso, fatalmente, daria ensejo à impunidade.

Neste diapasão, fica nítido perceber que não se cuida de analogia, a qual é vedada no Direito Penal, mas sim de interpretação progressiva. Esta, ao atualizar o Direito, dilata o "leque" de incidência da norma legal de modo a estabelecer sob o seu contorno fatos, que no momento social de sua elaboração não integravam o cotidiano da sociedade, e que, por isso, ficariam fora de seu alcance. Urge, pois, que o sentido da expressão "coisa móvel" expressa no *caput* do artigo 155 do Código Penal seja interpretada consoante o progresso da indústria (FELICIANO, 2001).

De qualquer modo, é de ser frisado que, para a seara penal, o substrato que se extrai das ilações lançadas acima reside em aspectos secundários, tais como:

> *[...] a mensuração de prejuízo (que tomará em conta a subtração de pelo menos 2 objetos materiais – o* hardware *e o* software *desde que não seja* shareware*),*[9] *para a dosimetria de certas penas restritivas de direito (nomeadamente, a prestação pecuniária de perda de bens e valores introduzidos pela Lei n.º 9.174/98), para a fixação de dias-multa (artigo 49, caput, c.c. artigo 89 do Código Penal – conseqüências do delito) e para verificação da reparação do dano (*e.g., *artigo 83, IV, do Código Penal) (FELICIANO, 2001, p. 53).*

Com referência ao furto qualificado, algumas hipóteses nos parecem admissíveis. Por exemplo, a qualificadora prevista para o concurso de pessoas também incidirá quando dois ou mais indivíduos conseguirem ingressar no sistema informático de uma determinada instituição financeira e, após violarem-no, transferirem valores para a conta corrente de um deles, repartindo, ao final, a importância auferida ilicitamente. Não se olvide que com referência à violação

9 Programa disponível publicamente para avaliação e uso experimental, sem custo de licenciamento. Trata-se, então, de um *software* de domínio público. Em geral, estipula-se prazo limitado de uso. Uma vez findo, deve-se recolher o pagamento referente à taxa de licenciamento.

de sistemas de segurança e senhas bancárias através de recursos informáticos, é cabível, também, o emprego da qualificadora prescrita para aquele que atuar na rapina com destreza, porquanto este termo designa habilidade apta a fazer com que a vítima não note a subtração (CASTRO, 2003).

Poderá, do mesmo modo, ser qualificado por escalada ou emprego de chave falsa naquelas ocasiões em que o agente, para adentrar no local onde se encontra o computador, valer-se de meios anormais (ARAS, 2001).

Imaginável, ainda, é a figura do furto de energia. Este, por sua vez, será admissível em duas situações: no uso desautorizado de *hardware*, visto que dessa conduta (furto de uso), apesar de atípica, decorrerá conseqüente consumo de energia elétrica. Entretanto, tal ação, inevitavelmente, esbarrará no princípio da insignificância, em face do valor irrisório do consumo de energia. A segunda hipótese a ser declinada é a relativa ao uso desautorizado da rede, com *Internet Protocol* alheio, visando a navegar ou efetuar ligações telefônicas através da WEB. Nesse evento, em particular, a interpretação progressiva do que prescreve o artigo 155, § 3.º do Código Penal é insofismável. Ademais, o uso desautorizado da rede nesses moldes, assemelha-se ao uso desautorizado de aparelho celular alheio, conduta esta que a doutrina e a jurisprudência têm definido como furto de energia (FELICIANO, 2001).

5.1.4 Dano

Exige-se, para a configuração do crime de dano, prejuízo econômico oriundo da destruição, inutilização ou deterioração da coisa alheia. Bem por isso, sujeito que enviar um vírus e destruir apenas *e-mails* de cunho emotivo ou amigável não praticará tal delito, vez que ausente o prejuízo econômico.

Neste passo, é de se gravar que a conduta daquele que deixa mensagem em uma *homepage*, "pichando" a página, não se subsume a norma prevista no artigo 163 do Código Penal. Ademais, consigne-se que embora a Lei nº. 9.605/98 tipifique a conduta do "pichador" ou do "grafiteiro", a punição se restringe aos atos de conspurcar quando estes são direcionados a edificações ou monumentos urbanos. Uma vez vedada a interpretação extensiva quando prejudicar o réu, conclui-se, infelizmente, que tal figura, ainda, permanece atípica (CASTRO, 2003).

Ainda nessa esteira, caso típico a ser trazido à baila é a ação danosa daquele que envia vírus de computador. Como sujeito ativo desse crime, tem-se, tão somente, aquele que disseminar o vírus. O seu criador, isto é, aquele que o projetou, não obstante o elevado grau de reprovabilidade da conduta, remanescerá à margem de legislação penal vigente.

Com referência à disseminação culposa de vírus, não se há cogitar em crime, uma vez que não há, em nosso ordenamento jurídico penal, previsão de dano culposo.

Relativamente a vírus que "acomete" um programa, prejudicando o desempenho do equipamento, considera-se consumado o delito de dano, visto que haverá, incontestavelmente, inutilização parcial ou deterioração da coisa. Vê-se, aqui, mais uma possibilidade de se aplicar a interpretação progressiva.

De outro lado, em se tratando de vírus enviado para computador da União, Estado, Município, empresa concessionária de serviços públicos ou sociedade de economia mista, deve-se aplicar a qualificadora prevista no inciso III, do parágrafo único do referido artigo. De igual modo, incidirá a qualificadora estabelecida pelo inciso IV, sendo o dano praticado por motivo egoístico ou em havendo prejuízo considerável para a vítima.

Por último, é interessante frisar que o delito de dano condiz com a classificação de crime de informática próprio ou puro, porquanto o agente visa a lesar, especificamente, o sistema de informática.

5.1.5 Estelionato

Os dizeres constantes do artigo 171 do Código Penal alcançam, potencialmente, "condutas desenvolvidas contra o computador e seus sistemas, ou por intermédio do computador e de seus sistemas" (FELICIANO, 2001, p. 75).

O comportamento, nessa conjuntura, consiste em o agente valer-se de meio fraudulento para induzir ou manter a vítima em erro, logrando com isso vantagem ilícita, para si ou para outrem. Isto posto, não é incomum a vítima ser lesada por estar exatamente utilizando, como recurso doméstico ou empresarial, os recursos concedidos pela informática.

Destas disposições vem a lume, pois, as fraudes informáticas. Vale advertir que o ambiente informático, nessa feição criminosa, ostenta determinadas peculiaridades que dificultam a coleta de provas, revelando-se, por isso, um interessante instrumento a serviço da delinqüência.

Como exemplo clássico de fraude informática, pode ser trazido o ingresso indevido no sistema bancário, mediante recurso informático, exprimido pela utilização de cartões de identificação ou senhas obtidos ilicitamente de clientes.

Neste evento, em particular, a indução em erro é indelével, vez que o banco autoriza a transferência por "acreditar" tratar-se de um cliente seu, o qual é identificado por uma senha ou outro dado qualquer passível de ser utilizado por outrem. Veja-se que, apesar do correntista não ter cognição instantânea da transferência ou saque na ocasião em que se efetua, a instituição financeira, através de seu sistema, trava ciência imediata e aprova a transação.

Neste sentido, questão que se antepõe diz respeito a uma curiosa questão, qual seja, a indução em erro na proposição supracitada atinge um sistema projetado pelo homem e não este. Entretanto, não resta dúvida de que, nessa situação, também é crível o expediente da interpretação progressiva (FELICIANO, 2001).

É de se atentar, contudo, que tal conduta difere daquela em que o agente, por ser um *expert* em sistemas de segurança digitais, consegue violar senhas bancárias e demais obstáculos apostos visando a coibir invasões desse jaez. O criminoso que, valendo-se dessa condição, logra transferir valores para certa conta corrente age com destreza, pois o êxito de sua ação decorre de sua própria habilidade. É esta que permite com que ele viole o sistema bancário, sem que seja percebido, isto é, durante todo o *iter criminis,* a instituição financeira não nota a violação do sistema. Portanto, não se há falar em ardil, artifício ou outro meio fraudulento qualquer, porquanto o que realmente se denota é apenas uma agilidade específica na área da informática, que possibilita o sucesso na empreitada criminosa. Ilustram tal suposição casos em que, em virtude da vulnerabilidade do sistema, o agente logra subtrair determinada quantia.

Por último, frise-se que, embora existam outros tipos penais passíveis de serem configurados através da utilização do computador, tais como os previstos nos artigos 208, 228, 286 e 287, todos do Código Penal, procuramos dissecar apenas alguns dos principais dispositivos aplicáveis aos crimes de informática. Finalmente arrematando, não poderiam cair no esquecimento algumas normas penais (sem prejuízo da existência de outras) de extrema evidência, pois de modo idêntico ao crime de dano, classificam-se, ainda que indiretamente, como crimes informáticos próprios ou puros: artigos 153, *caput* e parágrafo primeiro; 313-A; 313-B e 325.

6. CONDUTAS ATÍPICAS

Considerando-se o esboço anteriormente firmado, é irrefutável que as fórmulas e diretrizes das normas materiais penais nacionais, sobretudo o que representam em termos de "obsoletismo", têm sim notável proficuidade no combate à criminalidade na informática.

Todavia, a diminuta legislação sobre essa matéria, atrelada ao princípio da reserva legal, o qual, conforme já declinado, constitui-se em garantia fundamental, atuando como um setentrião para o Direito Penal, origina a atipicidade em algumas condutas praticadas por meio do computador.

O acesso não autorizado, indevido, ou ilegal à rede, sistema ou computador alheio trata-se de um comportamento que, ainda, não é emoldurado pela legislação penal e que, por conseguinte, não pode ser punido criminalmente (ROSA, 2002).

Outra conduta aviltante é a denominada sabotagem informática. Define-se como sendo a inserção, modificação, supressão ou extinção de dados, instruções ou programas de computador, ambicionando obstacularizar o funcionamento ou a capacidade de funcionamento de um sistema informático.

Sob esse mesmo prisma, também merece ser enfatizado o comportamento do indivíduo que cria e/ou aperfeiçoa a potencialidade lesiva de um vírus, o que, aliás, vem se expandindo com uma preocupante freqüência.

Da mesma forma, carecemos de uma previsão legal que vise a coibir a atuação daqueles que alteram, aniquilam ou inutilizam senhas indispensáveis ao funcionamento do sistema ou ao acesso à rede.

Outros exemplos dignos de menção são a "pichação" e o vandalismo na Internet. Aquele que insere algum texto ou imagem em *site* alheio, sem a devida permissão, até o presente momento não encontra freios em nossas leis penais (CASTRO, 2003).

Além disso, ecoa a ausência de tipicidade a conduta daquele que envia contínua, indevida e inadequadamente, através do correio-eletrônico, mensagens não solicitadas, que possibilitem assumir o controle da máquina do usuário vitimado.

Destarte, perante eventuais lacunas, é imperioso que venham a lume normas visando a proteger os bens jurídicos ligados à informática, criando assim, novos tipos penais aptos a extirparem a sensação de impunidade que tanto assola a sociedade, conquanto o Código Penal seja a *Magna Carta* do delinqüente *a contrario sensu:* tudo o que nele não está proibido é permitido, ressalvado, é óbvio, o estabelecido por leis esparsas.

7. DA NECESSIDADE DE "CRIMINALIZAÇÃO"

De início, é válido assinalar que a Internet pode e deve ser regulamentada pelo Estado brasileiro, haja vista que este, indubitavelmente, prega a inafastabilidade do controle jurisdicional.

De igual modo, no tocante às condutas ilícitas inéditas, a necessidade de o Estado evitá-las é manifesta, pois afetam de forma intolerável bens jurídicos que, embora ainda não estejam amparados, são, sem dúvida alguma, carecedores da tutela penal.

Por outro lado, não podemos perder de vista que apesar de as vitórias angariadas pela informática serem indubitavelmente revolucionárias, situam-se no plano instrumental dos meios e não no sublime patamar dos fins. É, pois, inadmissível qualquer exacerbação capaz de deturpar a ordem jurídica, de modo a afetar bens já amparados pelo Direito Penal e bens que, não obstante a ausência dessa proteção, são no contexto atual dignos de respaldo jurídico.

Feitos esses esclarecimentos, reputamos essencial adentrar, com a devida estima, na seara da "criminalização", bem como no âmbito legislativo, que permeiam o assunto em tela para, só então, tecermos um raciocínio coerente com o fito do presente esboço.

Considerando-se que não se há articular em dois mundos distintos, isto é, um "real", onde vigorariam as normas jurídicas e um "virtual", em que seria impossível o Estado intervir mediante a imposição de regras, é evidente a interação entre o progresso informático, principalmente no que se refere à Internet, e o Direito Penal. Ora, se a sociedade também convive no ciberespaço, neste também deverá operar o Direito.

Eis que surge, dentro dessa conjuntura, uma grande questão a ser expurgada: seria, realmente, imprescindível criminalizar as condutas que lesionem bens informáticos, tendo em vista que o Direito Penal é considerado a *ultima ratio,* a alternativa ao caos?

Hoje, podemos afirmar que o Direito Penal mostra-se, timidamente, desguarnecido para administrar a nova realidade da delinqüência. A desenvoltura com que a imaginação criminosa atua, pondo em prática a formatação profissional do crime, é de uma temeridade assaz.

Urge, pois, nestes dias inseguros, que o Direito Penal finque, definitivamente, suas balizas na ideologia da defesa social, a qual tem como foco central a segurança da comunidade.

Nesta senda, temos que o micro está para a criminalidade, assim como ele está para a sociedade de bem. A significar que, enquanto não impuserem limites, punindo essas condutas, até então atípicas, tal máquina será tão proveitosa para um homem de negócios quanto para um criminoso.

Ademais, é sabido que a impunidade propicia a evolução de toda e qualquer espécie de delinqüência. Destarte, é preocupante que esse poderoso instrumento esteja, pura e simplesmente, disponível para aqueles que possuem intenções avessas às prescrições do nosso ordenamento jurídico, sendo inconcebível permitir que descubram, efetivamente, a real envergadura desse novo "aliado", utilizando-o em sua integralidade para fins ilícitos.

Em suma, não significa, em hipótese alguma, promover o congestionamento de leis, tampouco anular a legislação penal existente. Neste sentido, vale invocar a preleção de José Paulo Sepúlveda Pertence, o qual. ao se deparar com a necessidade de avaliar as conseqüências do avanço tecnológico, assim pontificou:

> *[...] a invenção da pólvora não reclamou a definição do homicídio para tornar explícito que nela se compreendia a morte dada a outrem mediante arma de fogo" (HC. 76.689-PB, 1ª Turma do STF, Rel. Min. Sepúlveda Pertence, DJU de 6.11.1998, p. 3* apud *NALINI, 2004, p. 406).*

Todavia, ao lado do teor acima declinado, o qual certamente se aplica àquelas condutas que lesionem bens jurídicos já tutelados, onde a informática atua apenas como um novo instrumento ou *modus operandi* inovador, há outra

questão de crucial importância e que não pode ser descartada: a concepção de bem jurídico não pode ser estática, devendo estar aberta às mudanças sociais e aos progressos do conhecimento científico. Fala-se, então, em condutas inéditas, o que implica, necessariamente, uma ampliação da área acobertada pelo manto das normas penais. Daí, a necessidade de uma nova escrituração nesse sentido.

Por derradeiro, nesta mesma senda, impende destacarmos o Projeto de Lei nº 89/03 o qual, embora ainda se encontre em fase de tramitação pelo Congresso Nacional, prevê uma punição de três meses a um ano de detenção e multa para aquele que acessar indevidamente um meio eletrônico ou sistema informatizado. Pretende também o mesmo penalizar com detenção de seis meses a um ano e multa a conduta do indivíduo que fornecer, indevidamente ou sem autorização, informação obtida em meio eletrônico ou sistema informatizado.

8. CONCLUSÃO

A informática, como todo paradigma tecnológico, gera bônus e encargos, de modo que a nova era vivenciada, qual seja, a **era da informação** ou **infovia**, irrefragavelmente, revolucionou a conjuntura social sob diversos prismas.

O surgimento de um sistema de conexão mundial, como a Internet, além de atuar como expressiva ferramenta de labor, de entretenimento e de integração entre os povos, também fomentou a expansão de influxos maléficos à sociedade, cooperando não só para o declínio da decência humana, bem como conferiu certas "comodidades" a uma indigesta vertente social, representada pelos transgressores da ordem jurídica. Nesse aspecto, expressões como ***hackers, crackers, lammers, phreakers, insiders,*** dentre outras, passaram a definir uma nova gama de infratores.

Desta feita, coadjuvantes decorrentes dos avanços informáticos, tais como, o anonimato e o imediatismo, propiciaram não apenas novas formas de se cometerem delitos já definidos na lei penal, como também foram os responsáveis pelo surgimento de condutas inéditas, tidas como indesejáveis e carecedoras de tipificação.

Nasceu, assim, o crime de informática, conceituado como sendo toda conduta típica e antijurídica em que o meio de execução (**crime de informática impróprio**) ou o objeto juridicamente tutelado (**crime de informática próprio**) corresponda a um equipamento tecnológico.

Isto posto, é inarredável que, nesses casos, a aplicação do Direito Penal se faz necessária. Não se pode olvidar que, em face do princípio da inafastabilidade do controle jurisdicional, a jurisdição do Estado Democrático de Direito, indelevelmente, está presente nessa órbita. Portanto, todas as normas penais aplicáveis a qualquer indivíduo, desde que observado o preceito da reserva legal, também incidirá no âmbito virtual.

Assim, forçoso reconhecer que não se há cogitar, hodiernamente, na inaplicabilidade das normas constantes da Parte Especial do Código Penal brasileiro à criminalidade na informática, conquanto o fato constitutivo do delito se exprima na própria lei de modo exaustivo. Vale dizer, nesse ponto, quando ocorrer o preenchimento do requisito da tipicidade.

Ademais, recursos provenientes dos sistemas de interpretação, tal como, a interpretação histórico-evolutiva, cuja utilização visa a arrostar contextos de perplexidade em sede de criminalidade tecnológica, consubstanciam-se em um expediente juridicamente lídimo. Ressalte-se, ainda, que a lei é inteligível, a significar que o teor inserto no seu bojo deve acompanhar os avanços sociais, isto é, para que seja considerada eficaz, impende que a mesma caminhe concomitantemente com a realidade, sob pena de termos de criar, a cada dia, novos tipos penais.

Todavia, identificamos algumas condutas que, não obstante o alto grau de reprovabilidade social, permanecem como atípicas.

Bem por isso, quando se coloca em pauta o tema da tecnologia, aqui evidenciado pela informática, inevitavelmente retine a expressão **futuro** e, em se tratando de assegurar o porvir da humanidade, bem como a premência em retermos a impunidade que tanto nos aflige, conceitos como o de bem jurídico não podem obstacularizar a salvaguarda do direito.

Logo, no afã de afrontar as tarefas contemporâneas e também de possibilitar o maciço emprego dos benefícios oferecidos pela informática, sem maiores temores, faz-se mister uma reformulação nos instrumentos jurídico-penais, denotando que os dilemas inerentes ao século XXI não podem ser, devidamente, dirimidos mediante instrumentos intelectuais que permeavam o século XVIII.

Por derradeiro, é de suma relevância consignar que não se está aqui advogando a inflação legislativa.Antagonicamente, primamos por uma atividade legiferante parcimoniosa, atilada e diligente, conquanto de enunciação acessível ao leigo, exauriente no seu escopo e estritamente técnica.

A rigorosa aplicação da lei voltada aos fins sociais e às exigências do bem comum, os sistemas interpretativos e, primordialmente, o bom senso ético e científico acurado associados aos preceitos essenciais esculpidos pelo artigo 5º da Constituição Federal, são, indubitavelmente, ferramentas extraordinárias no que tange às distorções jurídicas impostas pela sociedade tecnológica. Contudo, não bastam para tanto. Embora exista a possibilidade de se aplicar, em vários casos, as normas incriminadoras previstas no Código Penal, urge, pois, que sejam preenchidas as lacunas existentes, para que se erradique a atipicidade de diversas condutas, socialmente reprováveis, relacionadas ao objeto informático.

REFERÊNCIAS

ARAS, Vladimir. *Crimes de informática: uma nova criminalidade.* Jus Navegandi, Teresina, a. 5, n. 51, out. 2001. Disponível em:<http://www1.jus.com.br/doutrina/texto.asp?id=2250>. Acesso em: 06 mar. 2004.

BARBOSA, Marco Antônio. O direito do passado e o futuro do direito. *Revista do curso de direito do centro universitário da FMU*, São Paulo, n. 25, p. 85-91, 2003.

BARROS, Lucivaldo Vasconcelos. *O crime na era da informação.* Jus Navegandi, Teresina, a. 7, n. 61, jan. 2003. Disponível em:<http://www1.jus.com.br/doutrina/texto.asp?id=3675>. Acesso em: 06 mar. 2004.

CASTRO, Carla Rodrigues de Araújo. *Crimes de informática e seus aspectos processuais.* 2.ed. Rio de Janeiro: Lúmen Júris, 2003.

COSTA, Marco Aurélio Rodrigues da. *Crimes de informática.* Jus Navegandi, Teresina, a. 1, n. 12, mai. 1997. Disponível em:<http://www1.jus.com.br/doutrina/texto.asp?id=1826>. Acesso em: 27 fev. 2004.

DELMANTO, Celso. et.al. *Código penal comentado.* 4.ed. Rio de Janeiro: Renovar, 1998.

FELICIANO, Guilherme Guimarães. *Informática e criminalidade: primeiras linhas.* Ribeirão Preto: Nacional de Direito, 2001.

FERREIRA, Ivette Senise. A criminalidade informática. In: LUCCA, Newton de; SIMÃO FILHO, Adalberto (Coords.). *Direito & internet: aspectos jurídicos relevantes.* Bauru: Edipro, 2001. cap. 7, p. 207-237.

FRANCO, Alberto Silva. et.al. *Código penal e sua interpretação jurisprudencial.* 5.ed.rev. e ampl. São Paulo: Revista dos Tribunais, 1995.

GOMES, A.L.C.N. *A informática como meio de execução dos crimes de furto, dano e estelionato.* Revista da Ajuris, São Paulo, n. 88, t. 1, p. 27-34, 2002.

GOMES, Luiz Flávio. Da política criminal paleorepressiva ao modelo político-criminal consensual. In:_____ *Suspensão condicional do processo penal: o novo modelo de justiça criminal.* São Paulo. Revista dos Tribunais, 1995. cap. 3, p. 55-81.

GRECO, M.A.; MARTINS, I.G.S. (Coords.). *Direito e internet: relações jurídicas na sociedade informatizada.* São Paulo: Revista dos Tribunais, 2001.

MIRABETE, Julio Fabbrini. *Manual de direito penal.* 17.ed. São Paulo: Atlas, 2001. v. 1.

MIRANDA, Marcelo Baeta Never. *Abordagem dinâmica aos crimes via internet.* Jus Navegandi, Teresina, a. 4, n. 37, dez. 1999. Disponível em:<http://www1.jus.com.br/doutrina/texto.asp?id=1828>. Acesso em: 06 mar. 2004.

MOREIRA, Rômulo de Andrade. *Globalização e crime.* Jus Navegandi, Teresina, a. 6, n. 53, jan. 2002. Disponível em: <http://www1.jus.com.br doutrina/texto.asp?id=2477>. Acesso em: 06 mar. 2004.

NALINI, José Renato. Perspectivas e desafios do direito penal no séc. XXI. In: SARTORI, Ivan Ricardo Garisio (Coord.). *Estudos de direito penal: aspectos práticos e polêmicos.* Rio de Janeiro: Forense, 2004. p. 373-409.

PAIVA, Mário Antônio Lobato de. *Os institutos do direito informático.* Jus Navegandi, Teresina, a. 6, n. 57, jul. 2002. Disponível em:<http://www1.jus.com.br doutrina/texto.asp?id=2571>. Acesso em: 06 mar. 2004.

PAIVA, Mário Antônio Lobato de. *Primeiras linhas em direito eletrônico.* Jus Navegandi, Teresina, a. 7, n. 61, jan. 2003. Disponível em:<http://www1.jus.com.br doutrina/texto.asp?id=3575>. Acesso em: 28 fev. 2004.

ROSA, Fabrizio.*Crimes de informática.* Campinas: Bookseller, 2002.

SILVA, José Geraldo da. O princípio da legalidade. In:_____ *Direito penal brasileiro.* São Paulo: Editora de Direito, 1996, cap. 8, p. 94-101.

SIQUEIRA, Paulo Hamilton. O direito na sociedade da informação. *Revista do curso de direito do centro universitário da FMU*, São Paulo, n. 25, p. 61-71, 2003.

WILLIAMS, Phil. *Crime organizado e cibercrime: sinergias, tendências e reações.* Revistas Eletrônicas. São Paulo, p. 1, 06 ago. 2001. Disponível em: <http://usinfo.state.gov/jornals/itgic/0801/ijgp/ig080108.htm>. Acesso em: 10 fev. 2004.